SAMWORTH CHURCH ACADEMY

DIOCESE OF SOUTHWELL & NOTTINGHAM MULTI ACADEMY TRUST

Bring your own Device (BYOD) Policy

Agreed by the MAT Board of Directors on 24 March 2020

Policy:	Bring your own device
Approved by:	SNMAT Board of Directors
Date:	March 2020
Review cycle:	Annual

VERSION CONTROL			
VERSION	DATE	AUTHOR	CHANGES
2020	March 2020	DO – I.T. Director	No changes

Agreed by the MAT Board of Directors on 24 March 2020

Bring Your Own Device (BYOD) Policy

Introduction

Bring Your Own Device (BYOD) is where a member of staff uses a personal computing device (laptops, tablets, smartphones or home PCs) for work purposes and/or to connect to the academy network. This might mean that a user's own devices are used to access personal data for which SNMAT has responsibility as data controller, as well as their own. BYOD raises a number of data protection concerns because the device is owned by the user rather than the data controller. The data controller must be able to demonstrate that it has secured, controlled or deleted all personal data on a particular device particularly in the event of a security breach.

Scope

This policy aims to ensure that:

- All processing of personal data which is under SNMAT control remains in compliance with the GDPR;
- Data is protected in the event of loss or theft of the device;
- Technical measures used to protect personal data remain proportionate to any benefits of BYOD.

This policy applies to devices owned by members of staff, directors/governors, and anyone else working in the academy. As a Trust SNMAT does not encourage the use of BYOD. However, where this is deemed necessary it should be authorised by the Headteacher and an acceptable use agreement signed by the member of staff/governor. A further policy would be required in the event of an academy introducing BYOD for students.

Rationale

The data protection legislation requires that personal data is "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')". This means SNMAT must have appropriate security in place to prevent the personal data it holds from being accidently or deliberately compromised. This is relevant if personal data is being processed on devices over which SNMAT may not have direct control.

As the Data Controller SNMAT therefore needs to give consideration to:

- what type of data is held;
- where data may be stored;
- how it is transferred;
- potential for data leakage;
- blurring of personal and business use;
- the device's security capacities;
- what to do if the person who owns the device leaves their employment; and
- how to deal with the loss, theft, failure and support of a device.

Agreed by the MAT Board of Directors on 24 March 2020

Roles and Responsibilities

Data Controller

The Diocese of Southwell and Nottingham Multi Academy Trust (SNMAT) is the corporate body registered with the Information Commissioners' Office as Data Controller. The Directors are ultimately accountable for implementation of the GDPR and must be able to demonstrate that they have secured, controlled or deleted all personal data on a particular device particularly in the event of a security breach.

Local Governing Bodies

Each of the academies within SNMAT is named on the data protection registration and the Board of Directors has delegated the responsibility for ensuring that all personal data on a particular device has been secured, controlled or deleted, particularly in the event of a security breach, to the Local Governing Bodies of the academies. The named Data Protection Governor, on behalf of the Local Governing Body, is responsible for monitoring the practice of Bring Your Own Device in the academy.

Principal/Headteacher

The Local Governing Body delegates the responsibility for dealing with 'day to day' management of issues in respect of BYOD to the Principal/Headteacher of the academy. He/she is responsible for:

- Authorising members of staff to use BYOD where appropriate;
- Ensuring that members of staff authorised to use their own devices have read and understood the BYOD Policy and signed the BYOD usage agreement;
- Ensuring staff authorised to use BYOD are informed that the academy may monitor their BYOD usage to ensure the security of any personal data;
- Ensuring that staff using their own device understand that failure to follow the policy may result in disciplinary action under the disciplinary procedure.

SNMAT Director of IT

To support the use of non-SNMAT/academy owned devices, the Director of IT will confirm IT support measures are in place at each academy to ensure that:

- SNMAT/the academy's minimum security measures are in place on the device, prior to being adding to the network. These include but are not limited to:

For tablets and smartphones –

- Must have a PIN code, shape code or biometrics to access the device.
- Must have the remote wipe capability enabled to ensure that, in the case of a lost device, possible data loss can be mitigated.
- Must not be shared with anyone outside of the academy.

For Windows or Mac devices –

- Must be password protected

Agreed by the MAT Board of Directors on 24 March 2020

- Must have separate profiles for different users (no shared profiles)
- Must have up to date and maintained Anti-Virus
- Must have full disk encryption enabled

- Action is taken to change passwords on the device if the device user informs SNMAT, the academy or the IT support provider of a possible password compromise;
- Only SNMAT/academy owned removable media that has been checked by IT support services, suitably encrypted and check for malware are to be used when connected to the academy network.

Staff

Where a member of staff has been authorised to use their own device for work purposes they are responsible for:

- ensuring no copies of trust data are made and/or stored on removable media, non-SNMAT owned devices or any non-SNMAT cloud based storage areas at any time;
- ensuring they only access trust data through a web browser using the online viewing and editing capabilities of the cloud service provider e.g. Office 365 or G-Suite and never using locally installed software such as Word, Excel, PowerPoint, Outlook or OneDrive for Business as these application cache data locally. (MAT agreed exceptions may apply on selected mobile devices)
- always logging off and disconnecting from the academy network when they have finished working;
- only accessing the SNMAT/academy's systems with their own name and registered password;
- keeping the passwords they use to access the SNMAT/academy's systems secure and secret;
- changing their passwords immediately if they believe they are no longer secure;
- informing SNMAT, the academy and IT support service as soon as possible if they believe their old password is no longer secure;
- ensuring that no one else has access to any sensitive data held on the device;
- referring to the Principal/Headteacher or Data Protection Officer if they are in any doubt as to the sensitivity of data they are using;
- always adhering to copyright;
- returning all data relating to SNMAT/the academy and destroying any locally or remotely held copies in non-SNMAT locations when they leave the employment of SNMAT;
- ensuring that when in the academy and not being used, the device must be kept in an office, locked room or drawer. It must never be left in an unlocked, unattended classroom;
- ensuring that, whenever possible, the device must not be left in an unattended car. If this cannot be avoided the device is to be locked in the boot;
- checking that the device is covered by their own insurance, whether in England or abroad;
- using any carrying case supplied with the device at all times when the device is being transported;
- where appropriate, ensuring the virus protection software that has been installed is kept up-to-date;
- ensuring that personally owned removable media is not used when connected to the network. Only SNMAT/academy owned removable media, which has been suitably

encrypted and checked, is to be used to access academy data. The loss of any trust owned removable media to be reported to SNMAT and the academy immediately;
- ensuring any and all software is fully licensed;
- ensuring that SNMAT/academy data is not accessed through an application that is not authorised by the MAT;
- ensuring the transfer of sensitive data is done using suitable encryption and following prescribed security principles as advised by SNMAT/the academy (ie Confidential information should not be put in the body of an email but either passed on using an agreed secure site/protocol or in an attached document that has been secured with a password. The password should be relayed to the recipient by some other means eg by phone or text, not using the same email address);

The Trust/the Academy reserves the right to refuse, prevent or withdraw access to Users and/or particular devices or software where it considers that there are unacceptable security, or other risks, to its staff, students, business, reputation, systems or infrastructure.

Objectives

The academy must ensure that:

- Procedures are in place for authorising staff to use BYOD;
- Usage agreements are in place for BYOD;
- Procedures are in place to protect personal data;
- Access to the academy's cloud hosted network/remotely accessed server is secure;
- Any data that is transferred to a device is done so as securely as is reasonably possible;
- Controls are in place to minimise the risk of introduction of viruses or malware to the academy network;

Links with Other Policies

The Bring Your Own Device (BYOD) Policy must be read in conjunction with the other following policies:

Data Protection Policy
ICT Guidance
Social Media
Records Management
E-Safety

Implementation

General principles

- SNMAT/the academy data should not be stored on or copied to non-trust devices or storage areas;
- Authorised non-trust owned devices should access trust data only through a web browser using the online viewing and editing capabilities of the cloud service provider, e.g. Office 365 or G-Suite, and never using locally installed software such as Word, Excel, PowerPoint, Outlook or OneDrive for Business as these applications cache data locally. (MAT agreed exceptions may apply on selected mobile devices)

Where personal data accessed by BYOD is stored either on the academy's cloud hosted network or a remotely accessible server the academy will ensure that:

- there is a strong password/pin/biometrics to secure the device;
- the application/device automatically locks if inactive for a period of time;
- the access credentials are secure in the event of loss or theft of a device e.g. does not permit the user to remain logged in between sessions;

The Trust/the Academy reserves the right to refuse, prevent or withdraw access to Users and/or particular devices or software where it considers that there are unacceptable security, or other risks, to its staff, students, business, reputation, systems or infrastructure.

Monitoring the Use of BYOD

The academy aims not to intrude into the private lives of staff. However, where the data being processed on personal devices is owned by SNMAT and, as the data controller, SNMAT is responsible for its security, SNMAT reserves the right to monitor the use of BYOD to ensure that the BYOD Policy is being complied with. Members of staff authorised to use BYOD will be required to sign an acceptable use statement, which agrees to this. The member of staff will be asked to provide their device for verifying for compliance purposes. Monitoring will only be carried out on the authorisation of the Principal/Headteacher and appropriate records will be kept, which can be accessed on request to the Principal/Headteacher (or the senior member of staff authorised by the Principal/Headteacher).

Penalties for breaches of data protection legislation have increased significantly under GDPR and disciplinary action will be taken against any employee who breaches any of the instructions or procedures following from the Data Protection Policy.

Review

This policy is reviewed annually by the Trust in consultation with the recognised trade unions. The application and outcomes of this policy will be monitored to ensure it is working effectively.

Agreed by the MAT Board of Directors on 24 March 2020

Appendix 1

Staff Acceptable BYOD Usage agreement

	Tick to confirm
I understand that no copies of trust data are to be made and/or stored on non-SNMAT or non-academy owned removable media, devices or cloud based storage areas at any time.	
I understand that when using a non-trust owned devices I will access trust data only through a web browser using the online viewing and editing capabilities of the cloud service provider eg Office 365 or G-Suite and never using locally installed software such as Word, Excel, PowerPoint, Outlook or OneDrive for Business. (MAT agreed exceptions may apply on selected mobile devices).	
I understand that no-one other than myself must ever have access to any sensitive data held (temporarily or otherwise) on the BYOD.	
I understand that I am responsible for the safety of any sensitive academy data that I use or access from my own device. If I am in any doubt as to the sensitivity of data I am using, I will refer to the Principal/Headteacher.	
I will always adhere to copyright.	
I will always log off and disconnect from the academy network when I have finished working.	
I will only access the academy's network with my own name and using my registered password. Passwords that I use to access academy systems will be kept secure and secret. If I have reason to believe my password is no longer secure, I will either change it immediately myself or ask the IT Support provider to make the change and inform the Principal/Headteacher and the IT support provider.	
When I leave the academy's employment I will ensure, all data relating to SNMAT/the academy held locally or remotely in non-SNMAT/academy locations are destroyed.	
I understand that when in the academy and not being used, the device must be kept in an office, locked room or drawer. It must never be left in an unlocked, unattended classroom.	
I understand that, whenever possible, the device must not be left in an unattended car. If this cannot be avoided the device will be locked in the boot.	
I will check that the device is covered by my own insurance, whether in England or abroad. I understand that when being transported an appropriate carrying case should be used for the device.	
I understand that I am responsible for ensuring that, where appropriate, virus protection software is installed and is kept up-to-date.	
I understand that I will not use personally owned removable media when connected to the academy's network. If directed/authorised to do so, I will only use SNMAT/academy owned removable media, which has been suitably encrypted and checked, to access academy data. Also I understand that data on this device should never be copied to the BYOD, but should be accessed directly from the removable media. I will report the loss of any such removable media device to SNMAT and the academy immediately.	

Agreed by the MAT Board of Directors on 24 March 2020

I understand that I will check with the academy's IT Support Service provider if I wish to install additional software onto the device to ensure it: • Is fully licensed; • Does not affect the integrity of the Trust/academy networks; • If not work related, does not access the school's data.	
I will always adhere to the following associated school policies: • Bring Your Own Device • Data protection • Social Media • ICT • E-safety • Records Management	
I understand that the Trust/academy may monitor my BYOD activity.	
I understand that activity that threatens the integrity of the academy's ICT systems, or activity that attacks or corrupts other systems, is forbidden.	
In order to maintain the security of data, I will take the following steps: • I will store data only for as long as is necessary for me to carry out my professional duties. • If I need to transfer sensitive data, I will only do so using encryption as advised by academy's IT Support Service provider. • I will not use email to transfer sensitive data but save them to the academy's cloud storage areas, if other staff need access to the information.	
I understand that if I do not adhere to these rules outlined in this agreement, my privilege of working with the BYOD could be suspended and other disciplinary consequences may follow, including notification to professional bodies, where appropriate. If an incident is considered to be an offence under the Computer Misuse Act or the Data Protection Act this may require investigation by the police and could be recorded on any future criminal record checks.	

Name _____ Signed _____

_____

Date _____

Authorised by _____ Principal/Headteacher

Date _____

Agreed by the MAT Board of Directors on 24 March 2020